

EV

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT14.06.00
04 AUG 2000

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年 5月23日

出 願 番 号
Application Number:

特願2000-151879

出 願 人
Applicant (s):

株式会社エヌ・ティ・ティ・ドコモ

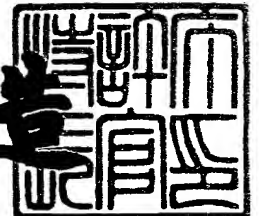
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 7月21日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3057552

【書類名】 特許願

【整理番号】 DCMH110358

【提出日】 平成12年 5月23日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【発明の名称】 通信システム、通信方法および通信ユニット

【請求項の数】 9

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ・ティ・ティ・ドコモ内

【氏名】 福本 雅朗

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ・ティ・ティ・ドコモ内

【氏名】 杉村 利明

【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社エヌ・ティ・ティ・ドコモ

【代理人】

【識別番号】 100098084

【弁理士】

【氏名又は名称】 川▲崎▼ 研二

【選任した代理人】

【識別番号】 100111763

【弁理士】

【氏名又は名称】 松本 隆

【選任した代理人】

【識別番号】 100108936

【弁理士】

【氏名又は名称】 秦 貴清

【手数料の表示】

【予納台帳番号】 038265

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信システム、通信方法および通信ユニット

【特許請求の範囲】

【請求項 1】 通信端末と、サーバとを具備し、

前記通信端末は、第 1 および第 2 の端末側通信手段を具備し、

前記サーバは、第 1 および第 2 のサーバ側通信手段を具備し、

前記通信端末の第 1 の端末側通信手段と前記サーバの第 1 のサーバ側通信手段は、インターネットを含まない 1 または複数の通信網を介して、秘匿を必要とする情報の通信を行い、

前記通信端末の第 2 の端末側通信手段と前記サーバの第 2 のサーバ側通信手段は、インターネットを含む 1 または複数の通信網を介して、秘匿を必要としない情報の通信を行う

ことを特徴とする通信システム。

【請求項 2】 通信端末と、サーバとを具備し、

前記通信端末は、第 1 および第 2 の端末側通信手段を具備し、

前記サーバは、第 1 および第 2 のサーバ側通信手段を具備し、

前記通信端末の第 1 の端末側通信手段と前記サーバの第 1 のサーバ側通信手段は、インターネットを含まない 1 または複数の通信網を介して、セッション鍵の交換を行い、

前記通信端末の第 2 の端末側通信手段と前記サーバの第 2 のサーバ側通信手段は、インターネットを含む 1 または複数の通信網を介して、前記セッション鍵によって暗号化された情報の通信を行う

ことを特徴とする通信システム。

【請求項 3】 通信端末が、第 1 の通信手段により、インターネットを含まない 1 または複数の通信網を介して、前記サーバとの間で、秘匿を必要とする情報の通信を行う過程と、

前記通信端末が、前記第 1 の通信手段とは別の第 2 の通信手段により、インターネットを含む 1 または複数の通信網を介して、前記サーバとの間で、秘匿を必要としない情報の通信を行う過程と、を具備する

ことを特徴とする通信方法。

【請求項 4】 通信端末が、第 1 の通信手段により、インターネットを含まない 1 または複数の通信網を介して、サーバとの間で、セッション鍵の交換を行う過程と、

前記通信端末が、前記第 1 の通信手段とは別の第 2 の通信手段により、インターネットを含む 1 または複数の通信網を介して、前記サーバとの間で、前記セッション鍵によって暗号化された情報の通信を行う過程と、を具備する

ことを特徴とする通信方法。

【請求項 5】 通信端末が、第 1 の通信手段により、インターネットを含む 1 または複数の通信網を介して、電子ショップサーバとの間で、商品の購買を行い、購入した商品を指定した購買タグを受信する過程と、

前記通信端末が、前記第 1 の通信手段とは別の第 2 の通信手段により、インターネットを含まない 1 または複数の通信網を介して、前記電子ショップサーバとの間で、前記購買タグおよび秘匿を必要とする個人情報の通信を行う過程と、

前記電子ショップサーバが、前記購買タグおよび個人情報を用いて決済を行う過程と、を具備する

ことを特徴とする通信方法。

【請求項 6】 通信端末が、第 1 の通信手段により、インターネットを含まない 1 または複数の通信網を介して、電子ショップサーバとの間で、セッション鍵の交換を行う過程と、

前記通信端末が、前記第 1 の通信手段とは別の第 2 の通信手段により、インターネットを含む 1 または複数の通信網を介して、前記電子ショップサーバとの間で、前記セッション鍵によって暗号化された情報で商品の購買を行い、購入した商品を指定した購買タグを記憶する過程と、

前記通信端末が、前記第 1 の通信手段により、インターネットを含まない 1 または複数の通信網を介して、前記電子ショップサーバとの間で、前記購買タグおよび秘匿を必要とする個人情報の通信を行う過程と、

前記電子ショップサーバが、前記購買タグおよび個人情報を用いて決済を行う過程と、を具備する

ことを特徴とする通信方法。

【請求項 7】 外部ユニットに装着されることによって通信端末を構成する通信ユニットであって、

インターネットを含まない 1 または複数の通信網に接続されるサーバの識別番号を記憶する記憶手段と、

前記識別番号を用いて前記サーバとの間で、インターネットを含まない 1 または複数の通信網を介した回線を接続する回線接続手段と、

前記回線を用いて秘匿を必要とする情報の通信を行う制御手段と、を具備することを特徴とする通信ユニット。

【請求項 8】 請求項 7 記載の通信ユニットにおいて、
前記秘匿を必要とする情報がセッション鍵である
ことを特徴とする通信ユニット。

【請求項 9】 請求項 7 記載の通信ユニットにおいて、
当該通信ユニットは、P C カードの形体を有する
ことを特徴とする通信ユニット。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、例えばインターネットのように秘匿性の保証されていないネットワーク上での通信に用いて好適な通信システム、通信方法および通信ユニットに関する。

【 0 0 0 2 】

【従来の技術】

近年、インターネットの普及に伴って、様々な情報通信がインターネット上で行われている。インターネット上で通信される情報には、ホームページのように広く一般に公開する目的を有する情報もあれば、例えば商取引や個人情報などのように秘匿を必要とする情報もある。

しかしながら、インターネットの通信プロトコルである T C P / I P (Transmission Control Protocol/Internet Protocol) そのものには、データの改竄や

盗聴を防ぐセキュリティの仕組みは備わっていないため、インターネットにおいて行う通信は秘匿性が保証されていないのが実情である。

そこで、秘匿を必要とする情報を通信する技術として、暗号通信技術があり、これを利用してインターネット上においても専用線と同様の安全性および利便性を有する通信を実現するものが提案されていた。

【 0 0 0 3 】

【発明が解決しようとする課題】

ところで、この暗号通信をインターネットに利用する場合において、暗号化および復号の際の演算量が少なく済む簡単な暗号を採用すると、暗号化および復号の処理負荷は少なくなるものの、第三者による暗号鍵の解読が容易に行われる可能性がある。その一方、十分な秘匿性を得るために複雑な暗号を採用すると、暗号化および復号の処理負荷が著しく高くなってしまい、迅速な通信を行うことが困難になる。このように、従来技術の下では、秘匿性を確保し、かつ、迅速に所望の相手と通信を行うことが困難であった。

【 0 0 0 4 】

本発明は、以上説明した事情に鑑みてなされたものであり、秘匿を必要とする情報の通信を高いセキュリティを維持し、かつ、迅速に行うことのできる通信システム、通信方法および通信ユニットを提供することを目的としている。

【 0 0 0 5 】

【課題を解決するための手段】

上述した課題を解決するため、請求項 1 記載の発明は、通信端末と、サーバとを具備し、

前記通信端末は、第 1 および第 2 の端末側通信手段を具備し、

前記サーバは、第 1 および第 2 のサーバ側通信手段を具備し、

前記通信端末の第 1 の端末側通信手段と前記サーバの第 1 のサーバ側通信手段は、インターネットを含まない 1 または複数の通信網を介して、秘匿を必要とする情報の通信を行い、

前記通信端末の第 2 の端末側通信手段と前記サーバの第 2 のサーバ側通信手段は、インターネットを含む 1 または複数の通信網を介して、秘匿を必要としない

情報の通信を行う

ことを特徴としている。

【0006】

請求項2記載の発明は、通信端末と、サーバとを具備し、

前記通信端末は、第1および第2の端末側通信手段を具備し、

前記サーバは、第1および第2のサーバ側通信手段を具備し、

前記通信端末の第1の端末側通信手段と前記サーバの第1のサーバ側通信手段は、インターネットを含まない1または複数の通信網を介して、セッション鍵の交換を行い、

前記通信端末の第2の端末側通信手段と前記サーバの第2のサーバ側通信手段は、インターネットを含む1または複数の通信網を介して、前記セッション鍵によって暗号化された情報の通信を行う

ことを特徴としている。

【0007】

請求項3記載の発明は、通信端末が、第1の通信手段により、インターネットを含まない1または複数の通信網を介して、前記サーバとの間で、秘匿を必要とする情報の通信を行う過程と、

前記通信端末が、前記第1の通信手段とは別の第2の通信手段により、インターネットを含む1または複数の通信網を介して、前記サーバとの間で、秘匿を必要としない情報の通信を行う過程と、を具備する

ことを特徴としている。

【0008】

請求項4記載の発明は、通信端末が、第1の通信手段により、インターネットを含まない1または複数の通信網を介して、サーバとの間で、セッション鍵の交換を行う過程と、

前記通信端末が、前記第1の通信手段とは別の第2の通信手段により、インターネットを含む1または複数の通信網を介して、前記サーバとの間で、前記セッション鍵によって暗号化された情報の通信を行う過程と、を具備する

ことを特徴としている。

【 0 0 0 9 】

請求項 5 記載の発明は、通信端末が、第 1 の通信手段により、インターネットを含む 1 または複数の通信網を介して、電子ショッピングサーバとの間で、商品の購買を行い、購入した商品を指定した購買タグを受信する過程と、

前記通信端末が、前記第 1 の通信手段とは別の第 2 の通信手段により、インターネットを含まない 1 または複数の通信網を介して、前記電子ショッピングサーバとの間で、前記購買タグおよび秘匿を必要とする個人情報の通信を行う過程と、

前記電子ショッピングサーバが、前記購買タグおよび個人情報を用いて決済を行う過程と、を具備する

ことを特徴としている。

【 0 0 1 0 】

請求項 6 記載の発明は、通信端末が、第 1 の通信手段により、インターネットを含まない 1 または複数の通信網を介して、電子ショッピングサーバとの間で、セッション鍵の交換を行う過程と、

前記通信端末が、前記第 1 の通信手段とは別の第 2 の通信手段により、インターネットを含む 1 または複数の通信網を介して、前記電子ショッピングサーバとの間で、前記セッション鍵によって暗号化された情報で商品の購買を行い、購入した商品を指定した購買タグを記憶する過程と、

前記通信端末が、前記第 1 の通信手段により、インターネットを含まない 1 または複数の通信網を介して、前記電子ショッピングサーバとの間で、前記購買タグおよび秘匿を必要とする個人情報の通信を行う過程と、

前記電子ショッピングサーバが、前記購買タグおよび個人情報を用いて決済を行う過程と、を具備する

ことを特徴としている。

【 0 0 1 1 】

請求項 7 記載の発明は、外部ユニットに装着されることによって通信端末を構成する通信ユニットであって、

インターネットを含まない 1 または複数の通信網に接続されるサーバの識別番号を記憶する記憶手段と、

前記識別番号を用いて前記サーバとの間で、インターネットを含まない１または複数の通信網を介した回線を接続する回線接続手段と、

前記回線を用いて秘匿を必要とする情報の通信を行う制御手段と、を具備することを特徴としている。

【 0 0 1 2 】

請求項 8 記載の発明は、請求項 7 記載の通信ユニットにおいて、前記秘匿を必要とする情報がセッション鍵であることを特徴としている。

【 0 0 1 3 】

請求項 9 記載の発明は、請求項 7 記載の通信ユニットにおいて、当該通信ユニットは、PC カードの形体を有することを特徴としている。

【 0 0 1 4 】

【発明の実施の形態】

[A. 第 1 実施形態]

＜A 1＞ 通信システムの構成

＜A 1 - 1＞ 通信システムの全体構成

まず、図 1 は本発明の第 1 実施形態に係る通信システムの構成例を示す模式図である。

この通信システムは、同図に示すように、通信端末 1 0 と、固定通信網 1 0 0 と、インターネット 2 0 0 と、移動通信網 3 0 0 と、サーバ 4 0 0 とによって大略構成されている。この通信システムにおいて、固定通信網 1 0 0 および移動通信網 3 0 0 は、盗聴などのおそれが比較的少なく安全性が高く、秘匿性が保証されているネットワークであるのに対して、インターネット 2 0 0 は盗聴などのおそれが比較的多く安全性が低く、秘匿性が保証されていないネットワークである。そこで、本実施形態では、移動通信網 3 0 0 を介して、通信端末 1 0 とサーバ 4 0 0 との間でセッション鍵の交換を行い、その後、固定通信網 1 0 0 およびインターネット 2 0 0 を介して、通信端末 1 0 とサーバ 4 0 0 との間で、このセッション鍵を用いた暗号通信を行う。

【 0 0 1 5 】

本実施形態では、暗号通信のための暗号化・復号方式として公開鍵暗号方式を採用し、セッション鍵として、この公開鍵暗号方式における公開鍵を使用する。

ここで、セッション鍵とは、1つのセッション（回線接続から回線接続断までの間）毎に使用される公開鍵のことである。

通信端末10およびサーバ400には、それぞれ複数の対をなす公開鍵と秘密鍵とが記憶されており、通信端末10およびサーバ400は、セッションの開始に先立って、互いにある公開鍵をセッション鍵として交換し、このセッション鍵に対応した秘密鍵を各自で保管する。

そして、セッションにおいて、通信端末10では、サーバ400から貰ったセッション鍵で暗号化した暗号信号を送信し、サーバ400側から受信した暗号信号を秘密鍵で復号する。一方、サーバ400では、通信端末10から貰ったセッション鍵で暗号化した暗号信号を送信し、通信端末10側から受信した暗号信号を秘密鍵で復号する。

このようなセッション鍵を用いた通信を通信端末10とサーバ400間で行うことにより、通信端末10およびサーバ400との間の通信に盗聴者が侵入するリプレーアタック等の不正が防止される。

【 0 0 1 6 】

〈A1-2. 通信端末の構成〉

通信端末10は、無線通信ユニットたる通信用PCカード50を外部ユニットたるパソコン11のカードスロット20に装着することにより構成されている（図2参照）。この通信端末10は、移動通信網300を介してサーバ400の第1ポート401に接続され、固定通信網100およびインターネット200を介してサーバ400の第2ポート402に接続されるものである。

【 0 0 1 7 】

図3は、パーソナルコンピュータ11（以下、パソコン11という）およびPCカード50の構成を示すブロック図である。

外部ユニットたるパソコン11は、図3に示すように、CPU12と、ROM（Read Only Memory）13と、RAM（Random Access Memory）14と、ハ

ードディスク装置15と、キー入力部16と、表示部17と、固定通信網100に接続されるモデム18と、カードスロット20の奥部に設けられたコネクタ19とによって大略構成されている。

ROM13は読み出し専用のプログラムメモリであり、CPU12はROM13から読出した制御プログラムを実行することにより、この通信端末10の各部を制御するものである。RAM14は、CPU12が各種制御プログラムを実行する際のワークエリアとして用いられる。

【0018】

ハードディスク装置15には、各種プログラムや、ユーザが利用する各種情報が記憶されている。

このハードディスク装置15に記憶されるプログラムには、例えば、パソコン11を固定通信網100を介してインターネット200に接続するダイヤルアッププログラム、移動通信網300を介して、PCカード50をサーバ400に接続するプログラム、固定通信網100およびインターネット200を介して、モデム18をサーバ400に接続するプログラム、暗号通信用プログラム等がある。

【0019】

ここで、ダイヤルアッププログラムとは、固定通信網100をインターネット200に接続する動作をCPU12に行わせるものである。具体的には、パソコン11を使用するユーザは、固定通信網100とインターネット200との間に接続されたプロバイダ（図示せず）に予め登録する。そして、固定通信網100とインターネット200とを接続するとき、通信端末10がこの登録の際に貰う送信ユーザID（例えば、〇〇〇△△）とパスワードをパソコン11に入力する。パソコン11のCPU12は、この送信ユーザIDおよびパスワードを、モデム18を介してプロバイダに送信する。プロバイダは、この送信ユーザIDとパスワードに基づいて認証処理を行い、固定通信網100をインターネット200に接続する。

暗号通信用プログラムとは、サーバ400にセッション鍵の交換要求、公開鍵の送信、この公開鍵に対応した秘密鍵の記憶、サーバ400から受信した公開鍵

(セッション鍵)の記憶、このセッション鍵を用いた情報の暗号化、受信した暗号信号の秘密鍵を用いた復号等、暗号通信に関する一連の動作をCPU12に行わせるものである。

また、ハードディスク装置15には、データテーブル15A(公開鍵(セッション鍵)POkey1~POkeynに対応した秘密鍵PSkey1~PSkeyn)(図5(a)参照)と、パソコン11のIPアドレスIPa、サーバ400のIPアドレスIPb等が各種情報として記憶されている。

なお、パソコン11は汎用のパーソナルコンピュータであり、PADでもよい。

【0020】

〈A1-3〉無線通信ユニット(PCカード)の構成

PCカード50は、記憶部51と、コントローラ52と、通信用送受信部53と、アンテナ54と、コネクタ55とによって大略構成されている。

【0021】

ここで、記憶部51は、メモリ51AおよびID記憶部51Bからなり、メモリ51Aには、コントローラ52で所定のオペレーティングシステムによりファイル管理を行うための汎用メモリの役割をなすエリアと、PCカードの制御プログラムが格納されたエリアとがある。

ここで、所定のオペレーティングシステムとは、メモリ51A内のデータを用いて汎用ファイル管理が可能なもの、例えばMS-DOS、MS-Windows、Mac OS又はUNIX(いずれも登録商標)などとして知られるオペレーティングシステムをいう。このようなオペレーティングシステムを用いる場合、PCカード50においては、通常の電話帳や電子メールのログファイル等は、ATAフラッシュディスク上の汎用ファイルとして、パソコン11により自由に読み書きが行われるものである。

また、ID記憶部51Bには、PCカード50の識別番号IDc(例えば電話番号)が記憶されると共に、サーバ400の識別番号IDb(電話番号)が記憶されている。

【0022】

コントローラ 52 は、メモリ 51 A に記憶された制御プログラムを実行するものである。このコントローラ 52 は、制御プログラムに従って、通信用送受信部 53 で受信された信号をコネクタ 55 に供給し、コネクタ 55 で受信された信号を通信用送受信部 53 に供給する。

【0023】

通信用送受信部 53 は、アンテナ 54 を介して移動通信網 300 に接続された基地局（図示せず）との間での通信が、例えば PDC (Personal Digital Cellular) 若しくは PHS (Personal Handyphone System) によって行われるものである。

【0024】

コネクタ 55 は、パソコン 11 のコネクタ 19 に接続される接続用コネクタである。

ここで、コネクタ 55 は、例えばコンパクトフラッシュ・タイプ II (Compact Flash Type II) のような汎用性の高いコネクタで、上述したパソコン 11、その他の外部情報機器と接続するための外部インターフェースを構成している。なお、PCカード 50 のコネクタ 55 は、上述のものに限定されるものではなく、PCカード・スタンダード (PC Card Standard) 等であってもよい。なお、PCカード・スタンダードとは、JEIDA (Japan Electronics Industry Development Association: 日本電子工業振興協会) と米国 PCMCIA (Personal Computer Memory Card International Association) が共同で制定した規格であり、厚さによって異なるタイプ I、タイプ II、タイプ III、タイプ IV 等がある。コンパクトフラッシュ (Compact Flash) ・タイプは更に小型で、タイプ II は縦横が 42.8×36.4 、厚さが $5.0(\text{mm})$ であり、これらをコネクタ 55 として採用することにより、PCカード 50 の小型化が容易となる。

【0025】

〈A1-4. サーバの構成〉

サーバ 400 は、図示しないルータを介してインターネット 200 に接続されると共に、図示しない基地局を介して移動通信網 300 に接続されたコンピュータである。

図4は、サーバ400の構成を示すブロック図である。サーバ400は、第1ポート401と、第2ポート402と、CPU403と、ROM404と、RAM405と、ハードディスク装置406とによって大略構成されている。

【0026】

第1ポート401は、図示しないアンテナ、通信用送受部等からなり、基地局を介して移動通信網300に接続されている。そして、この第1ポート401は、図1に示す如く、移動通信網300等を介して通信端末10に接続される。

【0027】

第2ポート402は、図示しないモデム、通信制御回路等からなり、ルータを介してインターネット200に接続されている。この第2ポート402は、図1に示す如く、インターネット200および固定通信網100等を介して通信端末10に接続される。

【0028】

ROM404は、制御プログラムを格納するプログラムメモリである。CPU403は、ROM404から読出した制御プログラムを実行することにより、サーバ400全体を制御するものである。この際、RAM405はCPU403のワークエリアとして用いられる。また、ROM404には、サーバ400の識別番号IDb（例えば電話番号）およびIPアドレスIPbが記憶されている。

【0029】

ハードディスク装置406は、情報記憶部406A、プログラム記憶部406Bおよび配信管理テーブル406Cという記憶エリアを有している。

情報記憶部406Aには、通信端末10に対して配信すべき情報を示す配信データが記憶される他、これらの情報のタイトルを通信端末10の表示部17に表示させるためのメニューデータ等が記憶されている。

【0030】

記憶されたデータには、文字や記号を示すテキストデータ、音声や楽曲を示す音楽データ、静止画や動画を示す画像データ、ゲームソフト等のコンピュータプログラム等がある。これらのデータは、例えば音楽データはMP3（MPEG Layer 3）形式、画像データはGIF（Graphics Interchange Format）形式、JPEG

(Joint Photographic Experts Group) 形式や M P E G (Moving Picture Experts Group) 形式で、それぞれ適当な圧縮方式にて圧縮されたものである。

【 0 0 3 1 】

プログラム記憶部 4 0 6 B には、情報配信プログラム、認証プログラム、移動通信網 3 0 0 を介して、第 1 ポート 4 0 1 を通信端末 1 0 の P C カード 5 0 に接続するプログラム、固定通信網 1 0 0 およびインターネット 2 0 0 を介して、第 2 ポート 4 0 2 を通信端末 1 0 のモデム 1 8 に接続するプログラムおよび暗号通信用プログラム等が格納されている。

【 0 0 3 2 】

ここで、情報配信プログラムとは、通信端末 1 0 から送信された要求情報に応じた配信情報の生成・送信を C P U 4 0 3 に行わせるものである。また、認証プログラムとは、配信管理テーブル 4 0 6 C に記憶されたユーザ I D、パスワード等に基づいてユーザ認証を C P U 4 0 3 で行わせるものである。

暗号通信用プログラムとは、通信端末 1 0 からセッション鍵の交換要求を受けた場合、公開鍵の送信、この公開鍵に対応した秘密鍵の記憶、通信端末 1 0 から受信した公開鍵（セッション鍵）の記憶、このセッション鍵を用いた情報の暗号化、受信した暗号信号の秘密鍵を用いた復号等、暗号通信に関する一連の動作を、C P U 4 0 3 に行わせるものである。

また、プログラム記憶部 4 0 6 B には、図 5 (b) に示すテーブルテーブル 4 0 6 D (公開鍵 (セッション鍵) S O k e y 1 ~ S O k e y n に対応した秘密鍵 S S k e y 1 ~ S S k e y n) 等が格納されている。

【 0 0 3 3 】

配信管理テーブル 4 0 6 C には、予め登録されたユーザ I D、パスワード等が格納されている。これらの情報は、受信されたユーザ I D およびパスワードと比較され、通信端末 1 0 (ユーザ) を特定するために用いられる。

【 0 0 3 4 】

＜ A 2 ＞ 第 1 実施形態の動作

次に、上記構成を有する実施形態の動作について説明する。

【 0 0 3 5 】

図6に示すシーケンスチャートを参照しながら、本実施形態の動作について説明する。

【0036】

まず、ユーザは、サーバ400との間で情報の送受信を行うため、パソコン11のキー入力部16に、サーバ400に予め登録したユーザIDおよびパスワード（以下、認証情報という）を入力する（ステップS1）。

【0037】

パソコン11のCPU12は、制御プログラムに従って、この認証情報をRAM14に記憶すると共に、認証情報をPCカード50に送信する。

PCカード50のコントローラ52は、メモリ51Aに記憶された制御プログラムに従って、サーバ400の識別IDbを送信先、PCカード50の識別番号IDcを送信元として認証情報に付加し、この情報を通信用送受信部53およびアンテナ54を介して基地局に送信する。これにより、ユーザIDおよびパスワードを含む情報は、移動通信網300を介してサーバ400側の基地局に送信され、この基地局から第1ポート401（サーバ400）に送信される（ステップS2）。

【0038】

サーバ400のCPU403は、認証情報を受けると、プログラム記憶部406Bに格納された認証プログラムを開始する。CPU403は、このプログラムに基づき、第1ポート401から受信された認証情報のユーザIDおよびパスワードに対して認証処理を行う（ステップS3）。

【0039】

ここで、CPU403は、受信されたユーザIDおよびパスワードが予め配信管理テーブル406Cに記憶されたものでなかった場合（ステップS3；NO）には、この処理を終了する（ステップS4）。

【0040】

一方、CPU403は、受信されたユーザIDおよびパスワードが予め配信管理テーブル406Cに記憶されたものであった場合（ステップS3；YES）には、許可信号がPCカード50（パソコン11）に送信される。パソコン11お

よびサーバ400は、互いに接続するプログラムを開始する。このプログラムに従って、PCカード50とサーバ400の第1ポート401との間に回線が張られ（ステップS5）、通信端末10がサーバ400に接続される。

【0041】

次に、パソコン11のCPU12は、ハードディスク装置15に記憶された暗号通信用プログラムが開始される。CPU12は、このプログラムに従って、セッション鍵の交換要求情報をPCカード50に向けて送信する。

PCカード50のコントローラ52は、制御プログラムに従って、サーバ400の識別番号IDbを送信先、PCカード50の識別番号IDcを送信元として交換要求情報に付加し、この情報を通信用送受信部53およびアンテナ54を介して基地局に送信する。これにより、交換要求情報は、移動通信網300（回線）を介してサーバ400に送信される（ステップS6）。

【0042】

パソコン11のCPU12は、暗号通信用プログラムに従って、ハードディスク装置15に格納されたデータテーブル15Aからある公開鍵POkey1をセッション鍵として選択し、このセッション鍵POkey1をPCカード50に向けて送信する。PCカード50のコントローラ52は、セッション鍵POkey1にサーバ400の識別番号IDbを送信先、PCカード50の識別番号IDcを送信元として付加し、この情報を回線を介してサーバ400に向けて送信する（ステップS7）。

また、サーバ400のCPU403は、交換要求情報を受けて、プログラム記憶部406Bに格納された暗号通信用プログラムが開始される。

CPU403は、このプログラムに従って、プログラム記憶部406Bに格納されたデータテーブル406Dからある公開鍵SOkey1をセッション鍵として選択し、このセッション鍵SOkey1にPCカード50の識別番号IDcを送信先、サーバ400の識別番号IDbを送信元として付加し、この情報を第1ポート401から移動通信網300（回線）を介してPCカード50に送信する（ステップS7'）。そして、PCカード50のコントローラ52は、サーバ400から送信されたセッション鍵SOkey1をパソコン11に送信する。

【0043】

パソコン11のCPU12は、回線およびPCカード50を介して受信したサーバ400のセッション鍵SOkey1をRAM14に記憶すると共に、送信したセッション鍵POkey1に対応した秘密鍵PSkey1をRAM14に記憶する（ステップS8）。

サーバ400のCPU403は、回線を介して受信したパソコン11のセッション鍵POkey1をRAM405に記憶すると共に、送信したセッション鍵SOkey1に対応した秘密鍵SSkey1を記憶する（ステップS9）。

【0044】

そして、パソコン10のCPU12は、セッション鍵の交換が完了すると、回線を切断する信号をサーバ400に送信し、回線の接続を切断する（ステップS10）。

【0045】

次に、通信端末10とサーバ400との間において、固定通信網100およびインターネット200を介して、秘匿を必要とする情報の授受する場合について説明する。

この処理に入る前に、前述したダイヤルアッププログラムを予め実行して固定通信網100をインターネット200に接続する。

次に、パソコン11のCPU12は、暗号通信用プログラムに従って、RAM14に記憶された認証情報（ユーザIDおよびパスワード）およびセッション鍵SOkey1を読み出し、この認証情報をセッション鍵SOkey1で暗号化し（ステップS11）、この暗号化した認証情報にサーバ400のIPアドレスIPbを送信先、パソコン11のIPアドレスIPaを送信元として付加し、この暗号化された認証情報、モデム18を介して固定通信網100に送信する。これにより、暗号化された認証情報は、固定通信網100およびインターネット200を介してサーバ400の第2ポート402に送信される（ステップS12）。

【0046】

サーバ400のCPU403は、暗号化された認証情報を受けると、暗号通信用プログラムに従って、RAM405に記憶された秘密鍵SSkey1を読み出し

、この秘密鍵 $SSkey1$ で暗号化された認証情報を複合する（ステップ $S13$ ）。

そして、CPU 403 は、認証プログラムに基づいて、復号された認証情報のユーザ ID およびパスワードに対して認証処理を行う（ステップ $S14$ ）。

【0047】

ここで、CPU 403 は、復号されたユーザ ID およびパスワードが予め配信管理テーブル $406C$ に記憶されたものでなかった場合（ステップ $S14$; NO）には、この処理を終了する（ステップ $S15$ ）。

【0048】

一方、CPU 403 は、復号されたユーザ ID およびパスワードが予め配信管理テーブル $406C$ に記憶されたものであった場合（ステップ $S14$; YES）には、許可信号がモデム 18 （パソコン 11 ）に送信される。パソコン 11 およびサーバ 400 は、互いに接続するプログラムを開始する。このプログラムに従って、モデム 18 とサーバ 400 の第 2 ポート 402 との間が、固定通信網 100 およびインターネット 300 を介して接続される。

【0049】

その後、通信端末 10 とサーバ 400 との間では、固定通信網 100 およびインターネット 300 を介して暗号通信による情報の授受を行う。

即ち、パソコン 11 の CPU 12 は、暗号通信用プログラムに基づいて、サーバ 400 に送信する情報を RAM 14 に記憶したセッション鍵 $SOkey1$ で暗号化し、サーバ 400 に送信する（ステップ $S17$ ）。一方、CPU 12 は、受信したサーバ 400 側からの暗号化された情報を、RAM 14 に記憶した秘密鍵 $PSkey1$ で復号する。

一方、サーバ 400 の CPU 403 は、暗号通信用プログラムに基づいて、パソコン 11 に送信する情報を RAM 405 に記憶したセッション鍵 $POkey1$ で暗号化し、通信端末 10 に送信する（ステップ $S17'$ ）。一方、CPU 403 は、受信したパソコン 11 側からの暗号化された情報を、RAM 405 に記憶した秘密鍵 $SSkey1$ で復号する。

これにより、通信端末 10 は、サーバ 400 の情報記憶部 $406A$ に記憶され

たデータをセキュリティを高めて受信する。

【0050】

そして、パソコン10のCPU12は、情報の授受が完了すると、通信を終了する（ステップS18）。これに伴って、パソコン11およびサーバ400にそれぞれ記憶されたセッション鍵および秘密鍵を消去し、セッション鍵および秘密鍵を無効にする。なお、セッション鍵および秘密鍵に寿命を持たせることにより、自動的に無効にするものであってもよく、この場合固定通信網100およびインターネット200の接続を切断することなしに、鍵を消去することも可能となる。

【0051】

〈A3〉第1実施形態の効果

以上、述べたように、本実施形態による通信システムでは、移動通信網300を介してセッション鍵の交換を行い、インターネット200および固定通信網100を介した通信時には、このセッション鍵を用いた暗号通信を行う。これにより、セキュリティの低いインターネット200を含む1または複数の通信網を介して通信を行う場合であっても、情報の秘匿性を高めることができる。

【0052】

[B. 第2実施形態]

次に、本発明による第2実施形態に係る通信システムについて説明する。本実施形態では、この通信システムを電子商取引（e-コマース：物品の購入）に適用した場合について述べる。

本実施形態の特徴は、秘匿を必要としない情報を固定通信網100およびインターネット200を含む通信網を用いて通信し、秘匿を必要とする情報をインターネットを含まない通信網を用いて通信した点にある。なお、本実施形態においては、前述した第1実施形態の通信システムとその基本構成が変わるところがないので、その説明を省略するものとする。

本実施形態におけるサーバ400は、電子商取引を行うために電子ショップサーバとなり、このサーバ400のハードディスク装置406には商品の情報や購買を行うためのプログラムが格納されることになる。

即ち、情報記憶部 4 0 6 A には、ユーザに対して販売する商品のメニューデータ、商品の情報データ等が記憶されている。なお、メニューデータとは、商品の写真や仕様等、各種情報および商品に対応した商品番号などである。

また、プログラム記憶部 4 0 6 B には、情報配信プログラム、認証プログラムの他、商品購買プログラムおよび決済処理プログラム等が格納される。

ここで、商品購買プログラムとは、ユーザ毎にバスケット番号 B 1 ~ B n を割り当て、このバスケット番号毎にユーザが購入を希望する商品の書き込みを、CPU 4 0 3 に行わせるものである。

決済処理プログラムとは、ユーザからクレジット番号や商品の送付先等の個人情報情報が送信された段階で、バスケットに書き込まれた商品の金額をクレジット会社等に請求する等を、CPU 4 0 3 に行わせるものである。

【 0 0 5 3 】

＜ B 1 ＞ 第 2 実施形態の動作

次に、上記構成を有する実施形態の動作について説明する。

【 0 0 5 4 】

図 7 に示すシーケンスチャートに基づき、本実施形態の動作について説明する。

まず、ユーザは、パソコン 1 1 に前述したダイヤルアッププログラムを行わせるために、送信ユーザ ID およびパスワードをキー入力部 1 6 から入力する。これにより、パソコン 1 1 の CPU 1 2 は、この送信ユーザ ID およびパスワードをプロバイダに送信し、固定通信網 1 0 0 がインターネット 2 0 0 に接続される。

【 0 0 5 5 】

また、本実施例では、送信ユーザ ID をサーバ 4 0 0 側での認証に用いるため、パソコン 1 1 の CPU 1 2 は、この送信ユーザ ID に、サーバ 4 0 0 の IP アドレス IP b を送信先、パソコン 1 1 の IP アドレス IP a を送信元として接続要求を固定通信網 1 0 0 およびインターネット 2 0 0 を介して送信する（ステップ S 2 1）。

【 0 0 5 6 】

ここで、サーバ400のCPU403は、プログラム記憶部406Bに格納された商品購買プログラムが実行される。CPU403は、このプログラムに基づき、送信ユーザIDに対応したバスケット番号B1を割り振り、RAM405に記憶する（ステップS22）。

【0057】

さらに、サーバ400のCPU403は、情報記憶部406Aのメニューデータを読み出し、このメニューデータにパソコンのIPアドレスIPaを送信先、サーバ400のIPアドレスIPbを送信元として付加し、この情報をインターネット200および固定通信網100を介してパソコン11に送信する（ステップS23）。

【0058】

パソコン11のCPU12は、受信したメニューデータを表示部17に表示する。これにより、ユーザはサーバ400が販売している商品を把握する。

ユーザは、パソコン11の表示部17のメニューを参照しつつ、所望の商品を選択する。即ち、ユーザが予め決められた選択動作を行うことにより、CPU12は、ユーザが選択した商品の番号（例えば、ddd）を固定通信網100およびインターネット200を介してサーバ400に送信する（ステップS24）。予め決められた選択動作とは、例えば、表示部17に表示される商品の写真をマウスのポインタでクリックする、といった具合である。そして、サーバ400のCPU403は、対応したバスケットB1に選択された商品番号dddを書き込む。

ユーザが商品の選択を終了すると、パソコン11に予め決められた信号がユーザによって入力されることにより、パソコン11のCPU12は、選択終了信号を固定通信網100およびインターネット200を介してサーバ400に送信する。

【0059】

サーバ400のCPU403は、この選択終了信号を受けて、送信ユーザIDに対応付けて購買タグ（バスケット番号B1+商品番号ddd）をRAM405に記憶する（ステップS25）。さらに、サーバ400のCPU403は、この

購買タグにパソコンのIPアドレスIPaを送信先、サーバ400のIPアドレスIPbを送信元として付加し、この情報を固定通信網100およびインターネット200を介してパソコン11に送信する（ステップS26）。

【0060】

パソコン11のCPU12は、この購買タグをRAM14に記憶する（ステップS27）。そして、パソコン10のCPU12は、商品の購買処理が終わると、固定通信網100およびインターネット200による通信を終了する（ステップS28）。

【0061】

次に、ユーザは、サーバ400にクレジット番号、商品の送信先住所等の個人情報を送信するために、パソコン11のキー入力部16に個人情報を入力する（ステップS29）。この個人情報とは、盗聴されては困る情報である。

【0062】

パソコン11のCPU12は、制御プログラムに従って、購買タグをRAM14から読出し、この購買タグをPCカード50に送信する。

PCカード50のコントローラ52は、メモリ51Aに記憶された制御プログラムに従って、サーバ400の識別番号IDbを送信先、PCカード50の識別番号IDcを送信元として購買タグに付加し、この情報を通信用送受信部53およびアンテナ54を介して基地局に送信する。これにより、購買タグは、移动通信網300を介してサーバ400側の基地局に送信され、この基地局から第1ポート401（サーバ400）に送信される（ステップS30）。

【0063】

サーバ400のCPU403は、購買タグを受けると、プログラム記憶部406Bに格納された認証プログラムが開始される。CPU403は、このプログラムに基づき、第1ポート401から受信された購買タグに対して認証処理を行う（ステップS31）。

【0064】

ここで、CPU403は、受信された購買タグがRAM405に記憶されたものでなかった場合（ステップS31；NO）には、この処理を終了する（ステッ

プS32)。

【0065】

一方、CPU403は、受信された購買タグがRAM405に記憶されたものであった場合(ステップS30;YES)には、許可信号がPCカード50(パソコン11)に送信される。パソコン11およびサーバ400は、互いに接続するプログラムを開始する。このプログラムに従って、PCカード50とサーバ400の第1ポート401との間に回線が張られ(ステップS33)、通信端末10がサーバ400に接続される。

【0066】

次に、パソコン11のCPU12は、制御プログラムに従って、個人情報をPCカード50に送信する。

PCカード50のコントローラ52は、メモリ51Aに記憶された制御プログラムに従って、サーバ400の識別IDbを送信先、PCカード50の識別番号IDcを送信元として個人情報に付加し、この情報を通信用送受信部53およびアンテナ54を介して基地局に送信する。これにより、個人情報は、移動通信網300を介してサーバ400側の基地局に送信され、この基地局から第1ポート401(サーバ400)に送信される(ステップS34)

【0067】

サーバ400のCPU403は、この個人情報を受けて、決済処理を行う(ステップS35)。この場合、クレジット会社に商品dddの金額を請求すると共に、商品dddを送信先住所に発送する手続き等を行う。

【0068】

そして、パソコン10のCPU12は、個人情報の送信等が終了すると、回線の接続を断つ信号をサーバ400に送信し、回線を切断する(ステップS36)

。

【0069】

<B2> 第2実施形態の効果

以上、述べたように、本実施形態による通信システムでは、固定通信網100およびインターネット200を介した通信によって商品の選択を行い、移動通信

網 2 0 0 を介した通信によって秘匿を必要とする個人情報を送信するようにした。これにより、盗聴者が個人情報を盗聴するのを防止でき、個人情報等の秘匿性を高めることができる。

【 0 0 7 0 】

〔 C . 第 3 実施形態 〕

次に、本発明による第 3 実施形態に係る通信システムについて説明する。本実施形態においては、この通信システムを電子商取引（ e - コマーズ：物品の購入）に適用した場合を例示する。

本実施形態の特徴は、インターネットを含まない通信網を介してセッション鍵の交換を行い、インターネットを含む通信網を介してこのセッション鍵を用いた通信を行い、最後に個人情報をインターネットを含まない通信網を介して通信した点にある。なお、本実施形態においては、前述した第 1 実施形態の通信システムとその構成は変わるところがないので、その説明を省略するものとする。

本実施形態におけるサーバ 4 0 0 は、電子商取引では電子ショッピングサーバなる。このため、サーバ 4 0 0 のハードディスク装置 4 0 6 には、商品の情報や購買を行うためのプログラムが格納されることになる。

即ち、情報記憶部 4 0 6 A には、ユーザに対して販売する商品のメニューデータ、商品の情報データ等が記憶されている。なお、メニューデータとは、商品の写真や仕様等、各種情報および商品に対応した商品番号などである。

また、プログラム記憶部 4 0 6 B には、情報配信プログラム、認証プログラムの他、商品購買プログラムおよび決済処理プログラム等が格納されている。

ここで、商品購買プログラムとは、ユーザ毎にバスケット番号 B 1 ~ B n を割り当て、このバスケット番号毎にユーザが購入を希望する商品の書き込みを、 C P U 4 0 3 に行わせるものである。

決済処理プログラムとは、ユーザからクレジット番号や商品の送付先等の個人情報が発信された段階で、バスケットに書き込まれた商品の金額をカード会社に請求書を発行する等を、 C P U 4 0 3 に行わせるものである。

【 0 0 7 1 】

〈 C 1 〉 第 3 実施形態の動作

次に、上記構成を有する実施形態の動作について説明する。

【0072】

図8および図9に示すシーケンスチャートを参照しながら、本実施形態の動作について説明する。

【0073】

まず、ユーザは、パソコン11のキー入力部16に、サーバ400に予め登録したユーザIDおよびパスワード（以下、認証情報という）を入力する（ステップS41）。

【0074】

パソコン11のCPU12は、制御プログラムに従って、この認証情報をRAM14に記憶すると共に、認証情報をPCカード50に送信する。

PCカード50のコントローラ52は、メモリ51Aに記憶された制御プログラムに従って、サーバ400の識別番号IDbを送信先、PCカード50の識別番号IDcを送信元として認証情報に付加し、この情報を通信用送受信部53およびアンテナ54を介して基地局に送信する。これにより、ユーザIDおよびパスワードを含む情報は、移動通信網300を介してサーバ400側の基地局に送信され、この基地局から第1ポート401（サーバ400）に送信される（ステップS42）。

【0075】

サーバ400のCPU403は、認証情報を受けると、プログラム記憶部406Bに格納された認証プログラムを開始する。CPU403は、このプログラムに基づき、第1ポート401から受信された認証情報のユーザIDおよびパスワードに対して認証処理を行う（ステップS43）。

【0076】

ここで、CPU403は、受信されたユーザIDおよびパスワードが予め配信管理テーブル406Cに記憶されたものでなかった場合（ステップS43；NO）には、この処理を終了する（ステップS44）。

【0077】

一方、CPU403は、受信されたユーザIDおよびパスワードが予め配信管

理テーブル406Cに記憶されたものであった場合（ステップS43；YES）には、許可信号がPCカード50（パソコン11）に送信される。パソコン11およびサーバ400は、互いに接続するプログラムを開始する。このプログラムに従って、PCカード50とサーバ400の第1ポート401との間にダイヤル回線が張られ（ステップS45）、通信端末10がサーバ400に接続される。

【0078】

次に、パソコン11のCPU12は、ハードディスク装置15に記憶された暗号通信用プログラムが開始される。CPU12は、このプログラムに従って、セッション鍵の交換要求情報をPCカード50に向けて送信する。

PCカード50のコントローラ52は、制御プログラムに従って、サーバ400の識別番号IDbを送信先、PCカード50の識別番号IDcを送信元として交換要求情報に付加し、この情報を通信用送受信部53およびアンテナ54を介して基地局に送信する。これにより、交換要求情報は、移動通信網300（回線）を介してサーバ400に送信される（ステップS46）。

【0079】

パソコン11のCPU12は、暗号通信用プログラムに従って、ハードディスク装置15に格納されたデータテーブル15Aからある公開鍵POkey1をセッション鍵として選択し、このセッション鍵POkey1をPCカード50に向けて送信する。PCカード50のコントローラ52は、セッション鍵POkey1にサーバ400の識別番号IDbを送信先、PCカード50の識別番号IDcを送信元として付加し、この情報を回線を介してサーバ400に向けて送信する（ステップS47）。

また、サーバ400のCPU403は、交換要求情報を受けて、プログラム記憶部406Bに格納された暗号通信用プログラムが開始される。

CPU403は、このプログラムに従って、プログラム記憶部406Bに格納されたデータテーブル406Dからある公開鍵SOkey1をセッション鍵として選択し、このセッション鍵SOkey1にPCカード50の識別番号IDcを送信先、サーバ400の識別番号IDbを送信元として付加し、この情報を第1ポート401から移動通信網300（回線）を介してPCカード50に送信する

(ステップS47')。

そして、PCカード50のコントローラ52は、サーバ400から送信されたセッション鍵SOkey1をパソコン11に送信する。

【0080】

パソコン11のCPU12は、回線およびPCカード50を介して受信したサーバ400のセッション鍵SOkey1をRAM14に記憶すると共に、送信したセッション鍵POkey1に対応した秘密鍵PSkey1をRAM14に記憶する(ステップS48)。

サーバ400のCPU403は、回線を介して受信したパソコン11のセッション鍵POkey1をRAM405に記憶すると共に、送信したセッション鍵SOkey1に対応した秘密鍵SSkey1を記憶する(ステップS49)。

【0081】

そして、パソコン10のCPU12は、セッション鍵の交換が完了すると、回線の接続を断つ信号をサーバ400に送信し、回線を切断する(ステップS50)。

【0082】

次に、前述した処理によって取得したセッション鍵を用いた暗号通信を固定通信網100およびインターネット200を介して行う。この処理に入る前に、前述したダイヤルアッププログラムを予め実行して固定通信網100をインターネット200に接続する。

次に、パソコン11のCPU12は、暗号通信用プログラムに従って、RAM14に記憶された認証情報(ユーザIDおよびパスワード)およびセッション鍵SOkey1を読み出し、この認証情報をセッション鍵SOkey1で暗号化し(ステップS51)、この暗号化した認証情報にサーバ400のIPアドレスIPbを送信先、パソコン11のIPアドレスIPaを送信元として付加し、この暗号化された認証情報を、モデム18を介して固定通信網100に送信する。これにより、暗号化された認証情報は、固定通信網100およびインターネット200を介してサーバ400の第2ポート402に送信される(ステップS52)。

【0083】

サーバ400のCPU403は、暗号化された認証情報を受けると、暗号通信用プログラムに従って、RAM405に記憶された秘密鍵SSkey1を読み出し、この秘密鍵SSkey1で暗号化された認証情報を複合する（ステップS53）。

そして、CPU403は、認証プログラムに基づいて、復号された認証情報のユーザIDおよびパスワードに対して認証処理を行う（ステップS54）。

【0084】

ここで、CPU403は、復号されたユーザIDおよびパスワードが予め配信管理テーブル406Cに記憶されたものでなかった場合（ステップS54；NO）には、この処理を終了する（ステップS55）。

【0085】

一方、CPU403は、復号されたユーザIDおよびパスワードが予め配信管理テーブル406Cに記憶されたものであった場合（ステップS54；YES）には、許可信号がモデム18（パソコン11）に送信される。パソコン11およびサーバ400は、互いに接続するプログラムを開始する。このプログラムに従って、モデム18およびサーバ400の第2ポート402とが、固定通信網100およびインターネット200を介して接続される。

【0086】

その後、通信端末10とサーバ400との間では、固定通信網100およびインターネット200を用いて暗号通信を行うことになる（ステップS57、S58、S60）。

【0087】

ここで、サーバ400のCPU403は、プログラム記憶部406Bに格納された商品購買プログラムを実行する。CPU403は、このプログラムに基づき、ユーザIDに対応したバスケット番号B1を割り振り、RAM405に記憶する（ステップS56）。

【0088】

さらに、サーバ400のCPU403は、情報記憶部406Aのメニューデータを読み出し、このメニューデータをセッション鍵POkey1で暗号化し、この

暗号化したメニューデータにパソコンのIPアドレスIPaを送信先、サーバ400のIPアドレスIPbを送信元として付加し、この情報を固定通信網100およびインターネット200を介してパソコン11に送信する（ステップS57）。

【0089】

パソコン11のCPU12は、受信したメニューデータを秘密鍵PSkey1で復号し、この復号したメニューデータを表示部17に表示する。これにより、ユーザはサーバ400が販売している商品を把握する。

ユーザは、パソコン11の表示部17のメニューを参照しつつ、所望の商品を選択する。即ち、予め決められた選択動作によって、ユーザが選択した商品の番号（例えば、ddd）を選択した場合、パソコン11のCPU12は、暗号通信用プログラムに従って、商品番号dddをセッション鍵SOkey1で暗号化し、この暗号化した商品番号にサーバ400のIPアドレスIPbを送信先、パソコン11のIPアドレスIPaを送信元として付加し、この暗号化された商品番号を、モデム18を介して固定通信網100に送信する。これにより、暗号化された商品番号は、固定通信網100およびインターネット200を介してサーバ400の第2ポート402に送信される（ステップS58）。

予め決められた選択動作とは、例えば、表示部17に表示される商品の写真をマウスのポインタでクリックする、といった具合である。

そして、サーバ400のCPU403は、暗号化された商品番号を受けると、暗号通信用プログラムに従って、RAM405に記憶された秘密鍵SSkey1を読み出し、この秘密鍵SSkey1で暗号化された商品番号を複合する。そして、CPU403は、復号された商品番号dddを、対応したバスケットB1に順次書き込む。

ユーザが商品の選択を終了すると、パソコン11に予め決められた信号がユーザによって入力されることにより、パソコン11のCPU12は、選択終了信号を固定通信網100およびインターネット200を介してサーバ400に送信する。

【0090】

サーバ400のCPU403は、この選択終了信号を受けて、ユーザIDに対応付けて購買タグ（バスケット番号B1+商品番号ddd）をRAM405に記憶する（ステップS59）。さらに、サーバ400のCPU403は、セッション鍵POkey1で暗号化し、この暗号化した購買タグにパソコンのIPアドレスIPaを送信先、サーバ400のIPアドレスIPbを送信元として付加し、この情報を固定通信網100およびインターネット200を介してパソコン11に送信する（ステップS60）。

【0091】

パソコン11のCPU12は、受信した購買タグを秘密鍵PSkey1で復号し、復号した購買タグをRAM14に記憶する（ステップS61）。そして、パソコン10のCPU12は、商品の購買処理が終わると、通信を終了する（ステップS62）。

【0092】

次に、ユーザは、サーバ400にクレジット番号、商品の送信先住所等の個人情報を送信するために、キー入力部16に個人情報を入力する（ステップS63）。この個人情報とは、盗聴されては困る情報である。

【0093】

パソコン11のCPU12は、制御プログラムに従って、購買タグをRAM14から読出し、この購買タグをPCカード50に送信する。

PCカード50のコントローラ52は、メモリ51Aに記憶された制御プログラムに従って、サーバ400の識別IDbを送信先、PCカード50の識別番号IDcを送信元として購買タグに付加し、この情報を通信用送受信部53およびアンテナ54を介して基地局に送信する。これにより、購買タグは、移動通信網300を介してサーバ400側の基地局に送信され、この基地局から第1ポート401（サーバ400）に送信される（ステップS64）。

【0094】

サーバ400のCPU403は、購買タグを受けると、プログラム記憶部406Bに格納された認証プログラムが開始される。CPU403は、このプログラムに基づき、第1ポート401から受信された購買タグに対して認証処理を行う

(ステップS65)。

【0095】

ここで、CPU403は、受信された購買タグがRAM405に記憶されたものでなかった場合(ステップS65; NO)には、この処理を終了する(ステップS66)。

【0096】

一方、CPU403は、受信された購買タグがRAM405に記憶されたものであった場合(ステップS65; YES)には、許可信号がPCカード50(パソコン11)に送信される。パソコン11とサーバ400の間には、移動通信網300を介してダイヤル回線が張られ(ステップS67)、通信端末10がサーバ400に接続される。

【0097】

次に、パソコン11のCPU12は、制御プログラムに従って、個人情報をPCカード50に送信する。

PCカード50のコントローラ52は、メモリ51Aに記憶された制御プログラムに従って、サーバ400の識別IDbを送信先、PCカード50の識別番号IDcを送信元として個人情報に付加し、この情報を通信用送受信部53およびアンテナ54を介して基地局に送信する。これにより、個人情報は、移動通信網300を介してサーバ400側の基地局に送信され、この基地局から第1ポート401(サーバ400)に送信される(ステップS68)

【0098】

サーバ400のCPU403は、この個人情報を受けて、決済処理を行う(ステップS69)。この場合、クレジット会社に商品dddの金額を請求すると共に、商品dddを送信先住所に発送する手続き等を行う。

【0099】

そして、パソコン10のCPU12は、個人情報の送信等が終了すると、ダイヤル回線の接続を断つ信号をサーバ400に送信し、回線を切断する(ステップS70)。

【0100】

〈C 2〉第 3 実施形態の効果

以上、述べたように、本実施形態による通信システムでは、固定通信網 1 0 0 およびインターネット 2 0 0 を介して商品の選択を行う場合、予めセキュリティの高い移動通信網 3 0 0 を介してセッション鍵を交換し、このセッション鍵を用いて固定通信網 1 0 0 およびインターネット 2 0 0 を介した通信を行うようにした。これにより、盗聴者が個人情報を盗聴するのを防止でき、個人情報等の秘匿性を高めることができる。

しかも、本実施形態では、固定通信網 1 0 0 およびインターネット 2 0 0 による通信をセッション鍵によって暗号化して行っているため、購買タグを盗聴者が盗聴するのを防止でき、同じ製品を先回りして買われてしまうのを防止することができる。また、この方式は、1 つの製品を買うオークション等の場合に、特に有効である。

【0 1 0 1】

[D. 変形例]

〈D-1〉

前記各実施形態では、固定通信網 1 0 0 およびインターネット 2 0 0 を介して秘匿を必要としない情報の通信を行い、移動通信網 3 0 0 を介して秘匿を必要とする情報の通信を行うようにしたが、本発明はこれに限らず、図 1 0 に示すように、固定通信網 1 0 0 およびインターネット 2 0 0 を介して秘匿を必要としない情報の通信を行い、移動通信網 3 0 0 および固定通信網 1 0 0 を介して秘匿を必要とする情報の通信を行うにしもよく、また図 1 1 に示すように、移動通信網 3 0 0 およびインターネット 2 0 0 を介して秘匿を必要としない情報の通信を行い、移動通信網 3 0 0 を介して秘匿を必要とする情報の通信を行うにしてもよい。

【0 1 0 2】

〈D-2〉

前記第 1、第 3 実施形態では、固定通信網 1 0 0 およびインターネット 2 0 0 で暗号通信を行う場合、1 個のセッション鍵を用いて暗号化するようにしたが、2 個以上のセッション鍵をダイヤル回線を用いて交換し、これらのセッション鍵によって暗号化することも可能である。

【0103】

<D-3>

前記第2、第3実施形態では、購買タグがサーバ400から通信端末10に送信された後に、固定通信網100およびインターネット200を介した通信を終了するようにしていたが、終了した後でも、一定時間内に通信端末10側から購買タグがサーバ400に向けて送信されることにより、商品の追加、削除等の変更を可能としてもよい。この場合には、個人情報ユーザから入力されるまでの間、この処理を可能にしてもよく、またタイマを作動させてこの処理を行わせるようにしてもよい。

【0104】

<D-4>

前記各実施形態における通信は、例えばパケット通信方式によって行うようにしてもよい。

【0105】

<D-5>

前記無線端末10は、パソコン11のカードスロット20にPCカード50を装着することによって構成したが、本発明はこれに限らず、パソコン11に携帯電話またはPHSを接続したものであってもよい。本発明を構成する通信端末は2つの通信手段を備えたものであればよい。

【0106】

【発明の効果】

上述したように本発明によれば、秘匿を必要とする情報の通信を高いセキュリティを維持し、かつ、迅速に行うことができる。

【図面の簡単な説明】

【図1】

本発明の第1実施形態に係る通信システムの概略構成を示すブロック図である。

【図2】

同実施形態に係る通信端末を構成するパソコンと無線通信ユニット（PCカー

ド) とを示す斜視図である。

【図 3】

同実施形態に係るパソコンおよび PC カードの概略構成を示すブロック図である。

【図 4】

同実施形態に係るサーバの構成の概略構成を示すブロック図である。

【図 5】

同実施形態に用いられるセッション鍵に対する秘密鍵を示したデータテーブルである。

【図 6】

同実施形態による通信システムの動作を示すシーケンスチャートである。

【図 7】

第 2 実施形態による通信システムの動作を示すシーケンスチャートである。

【図 8】

第 3 実施形態による通信システムの動作を示すシーケンスチャートである。

【図 9】

同実施形態による通信システムの動作を示す図 8 に続くシーケンスチャートである。

【図 10】

本発明の変形例による通信システムの概略構成を示すブロック図である。

【図 11】

本発明の他の変形例による通信システムの概略構成を示すブロック図である。

【符号の説明】

- 10・・・通信端末
- 11・・・パソコン
- 18・・・モデム
- 50・・・PCカード
- 100・・・固定通信網
- 200・・・インターネット

3 0 0 . . . 移動通信網

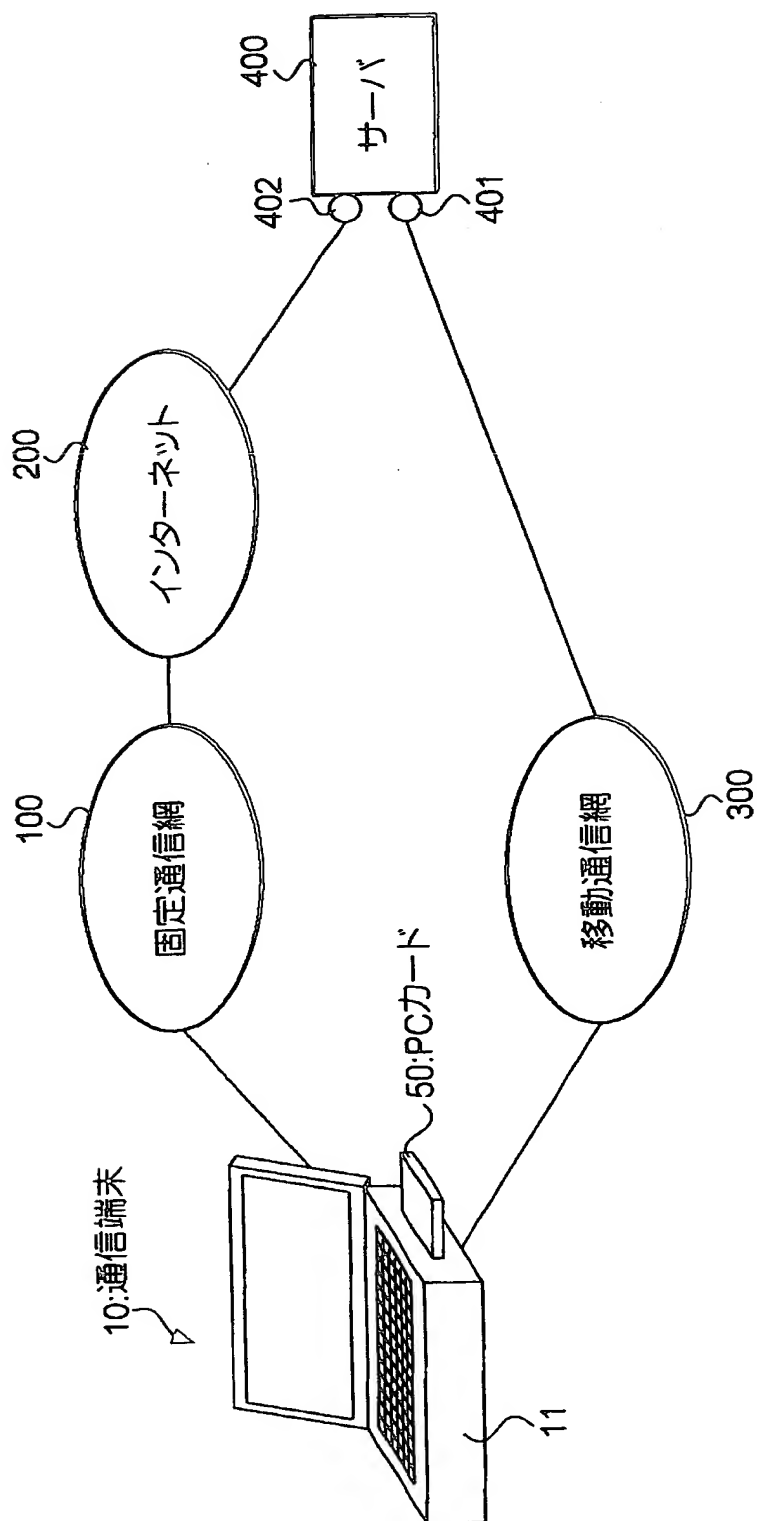
4 0 0 . . . サーバ

4 0 1 . . . 第 1 ポート

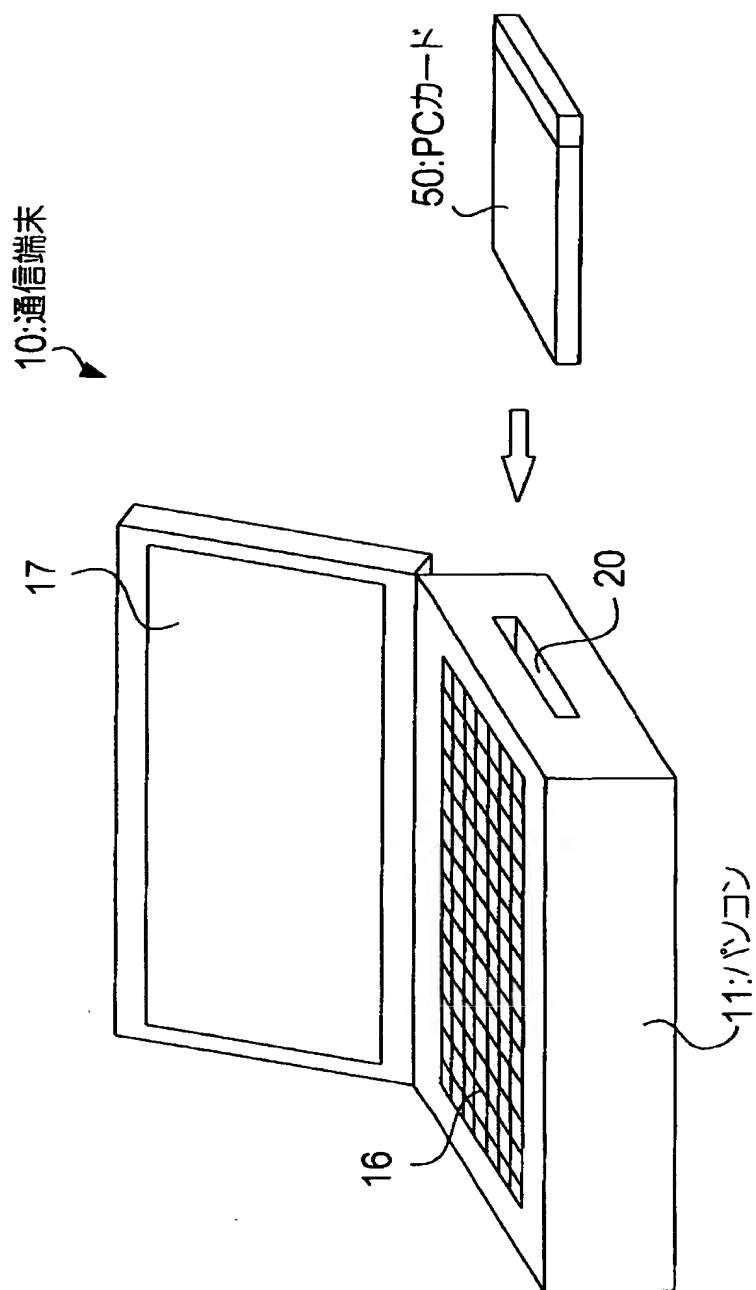
4 0 2 . . . 第 2 ポート

【書類名】 図面

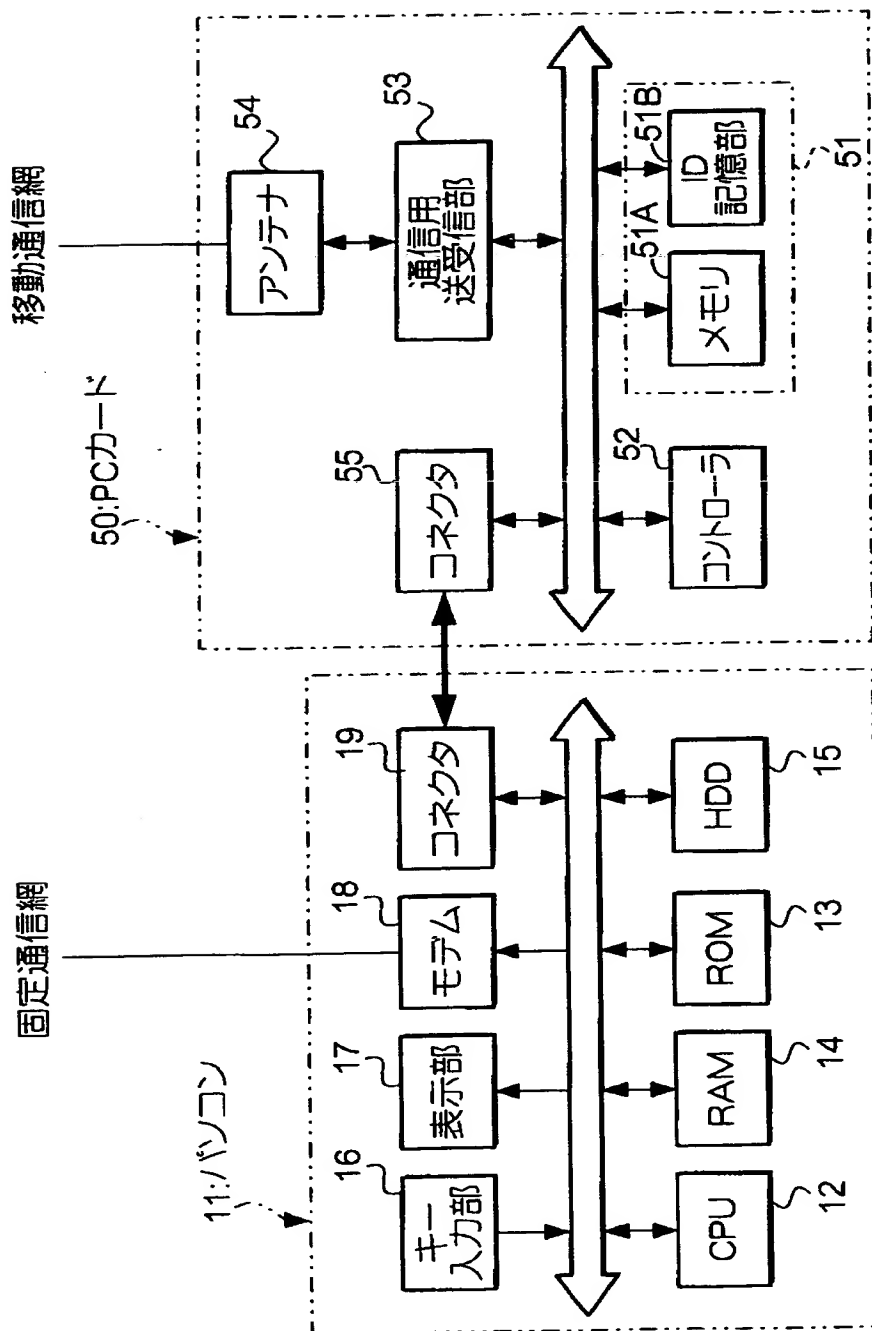
【図 1】



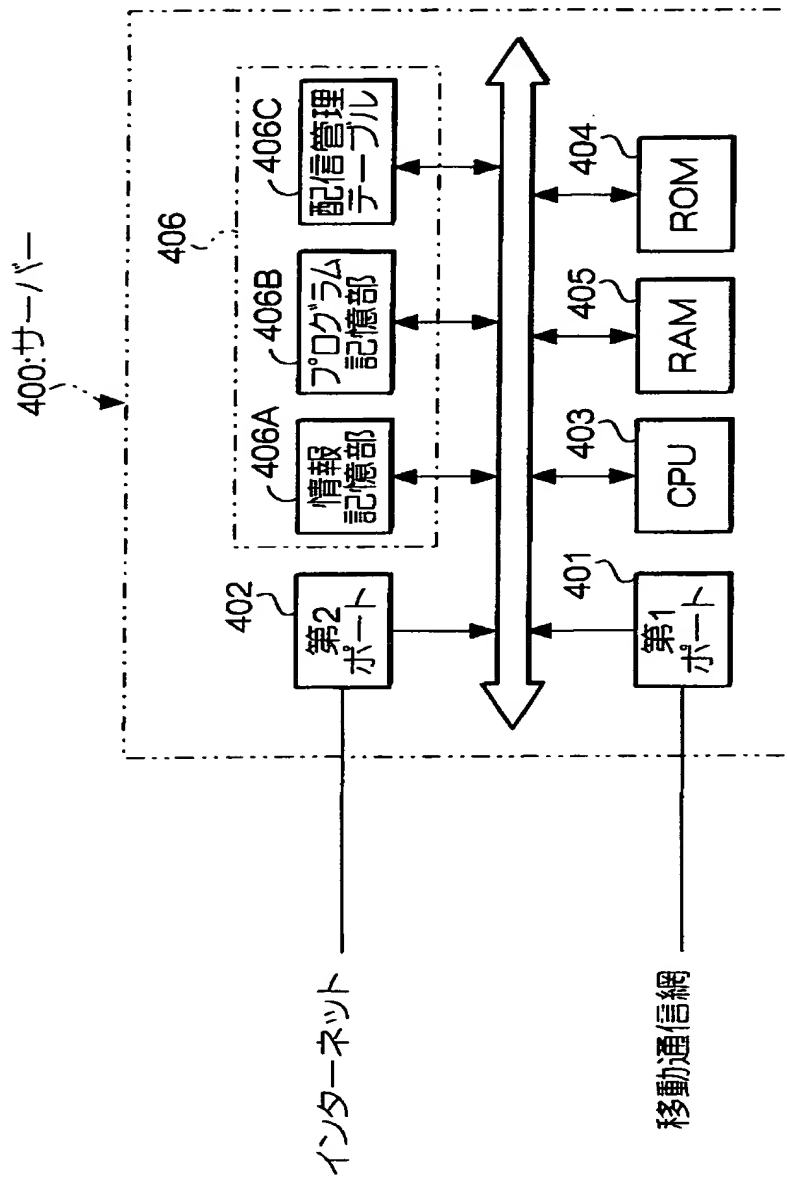
【図 2】



【図 3】



【図4】



【図 5】

(a)

15A

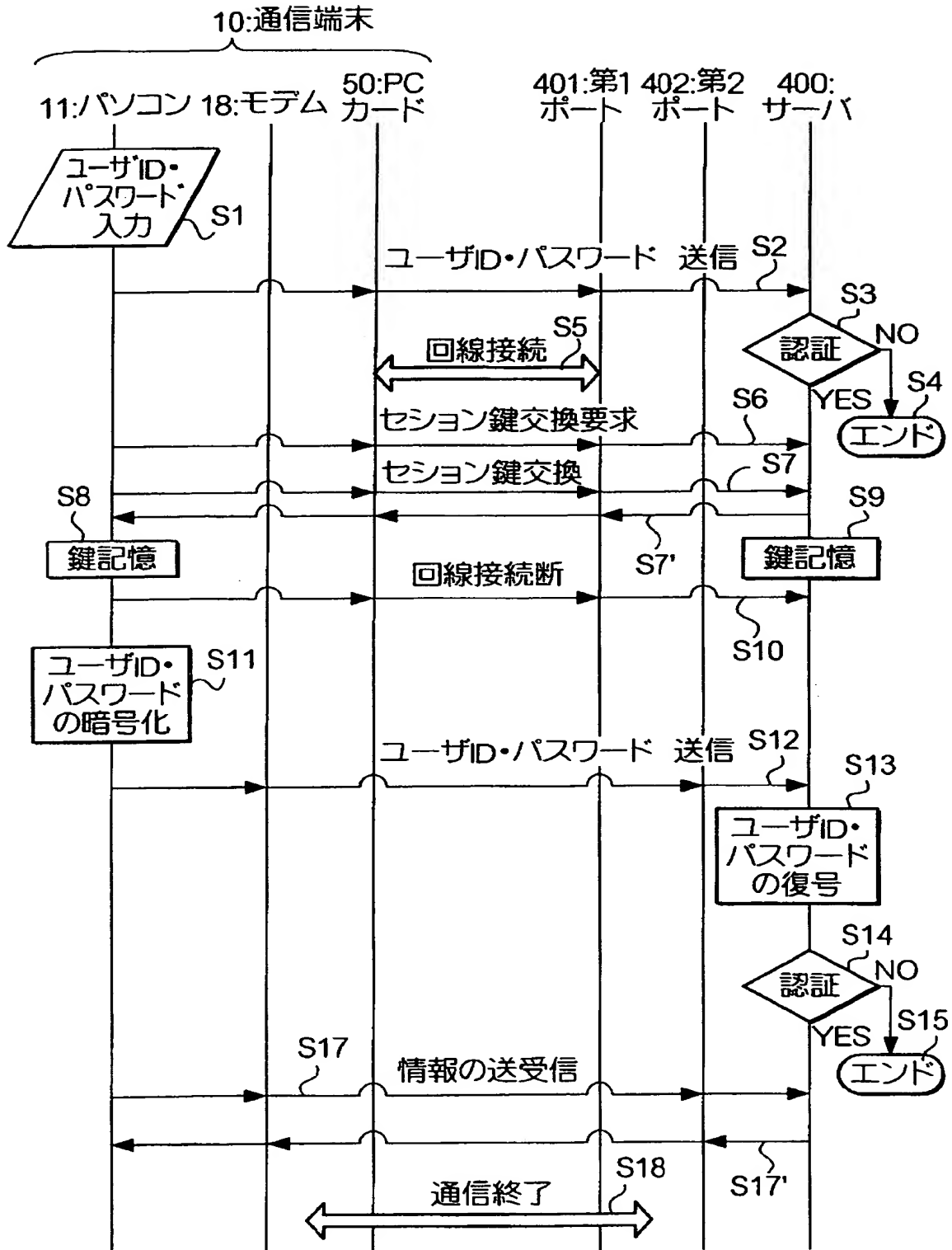
公開鍵 (セッション鍵)	秘密鍵
POkey1	PSkey1
POkey2	PSkey2
⋮	⋮
POkeyn	PSkeyn

(b)

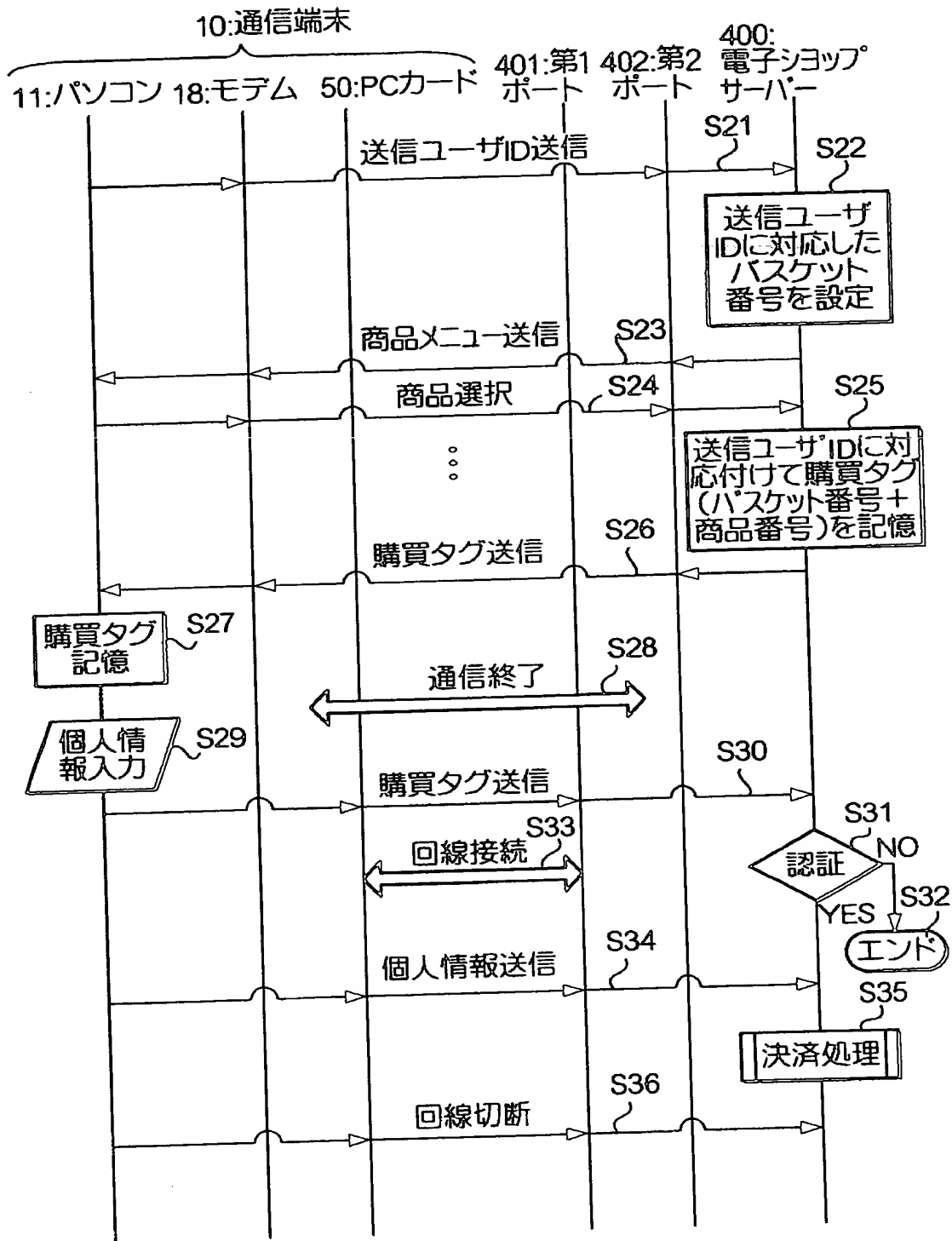
406D

公開鍵 (セッション鍵)	秘密鍵
SOkey1	SSkey1
SOkey2	SSkey2
⋮	⋮
SOkeyn	SSkeyn

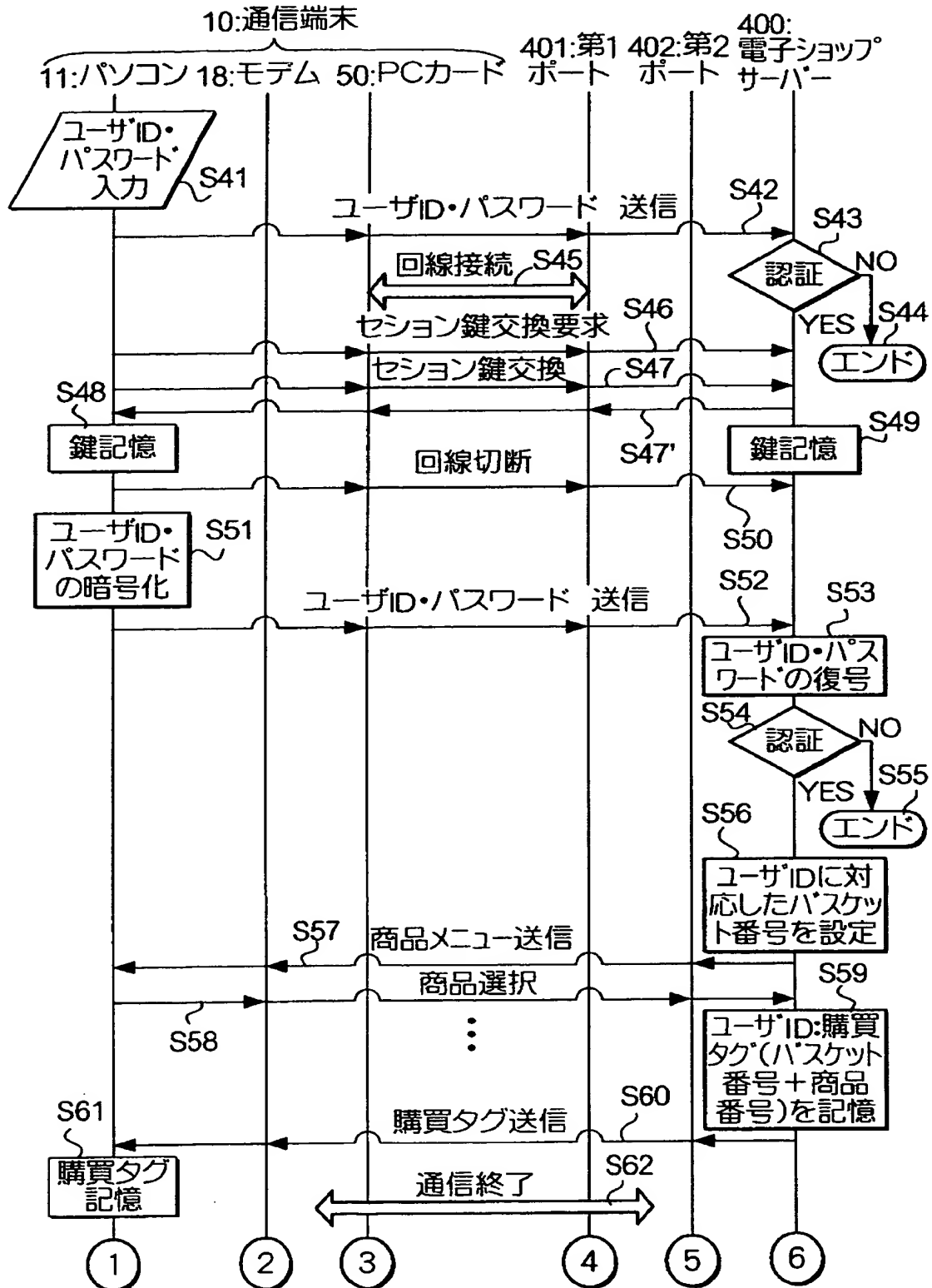
【図6】



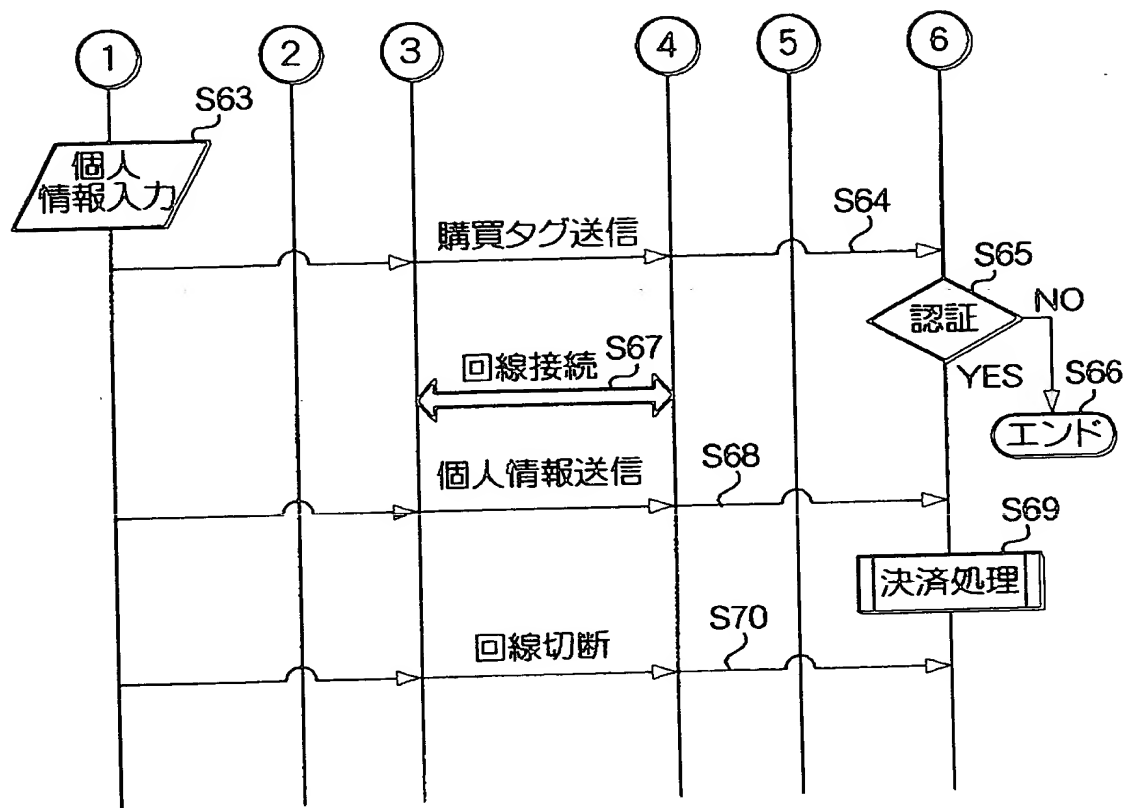
【図7】



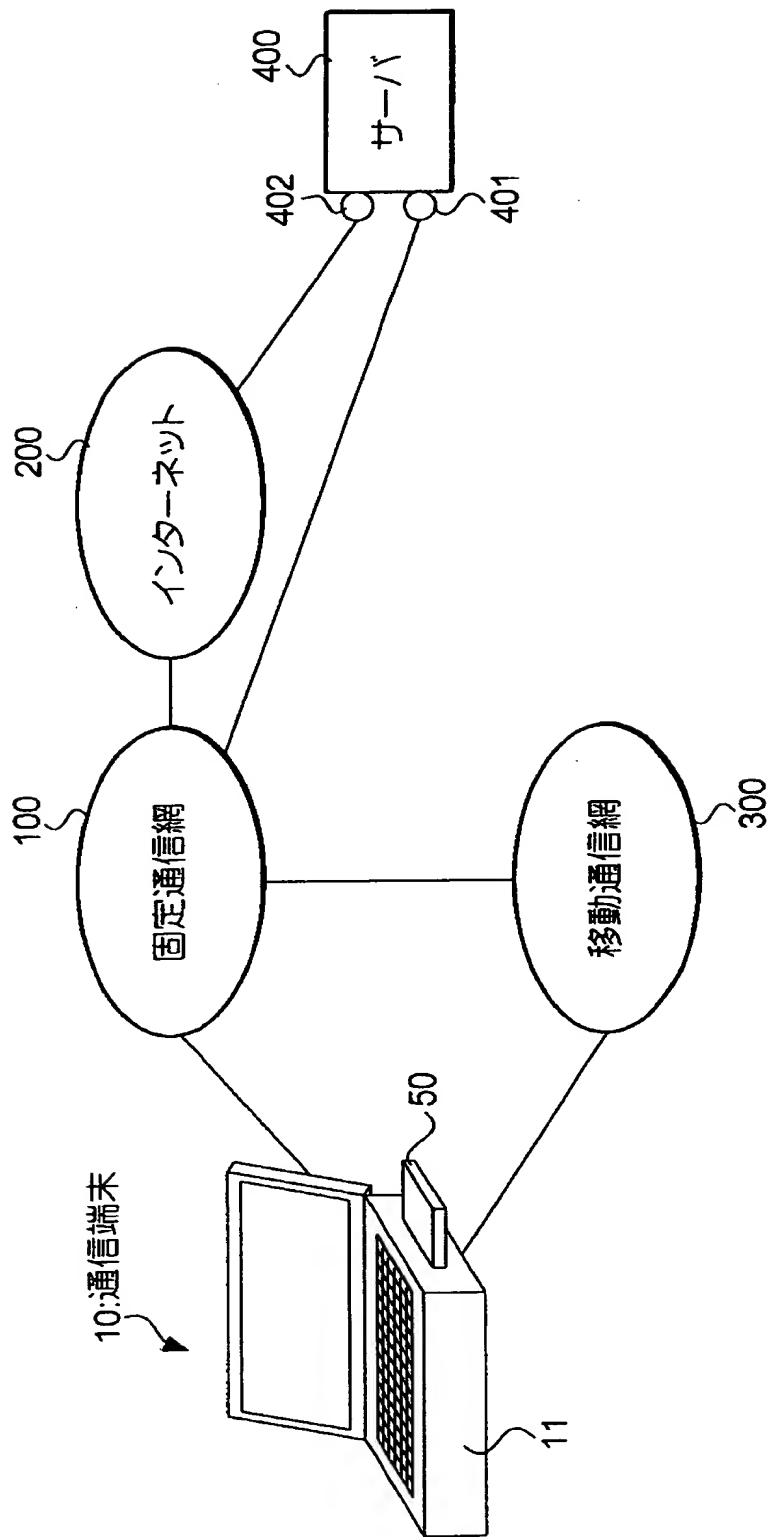
【図 8】



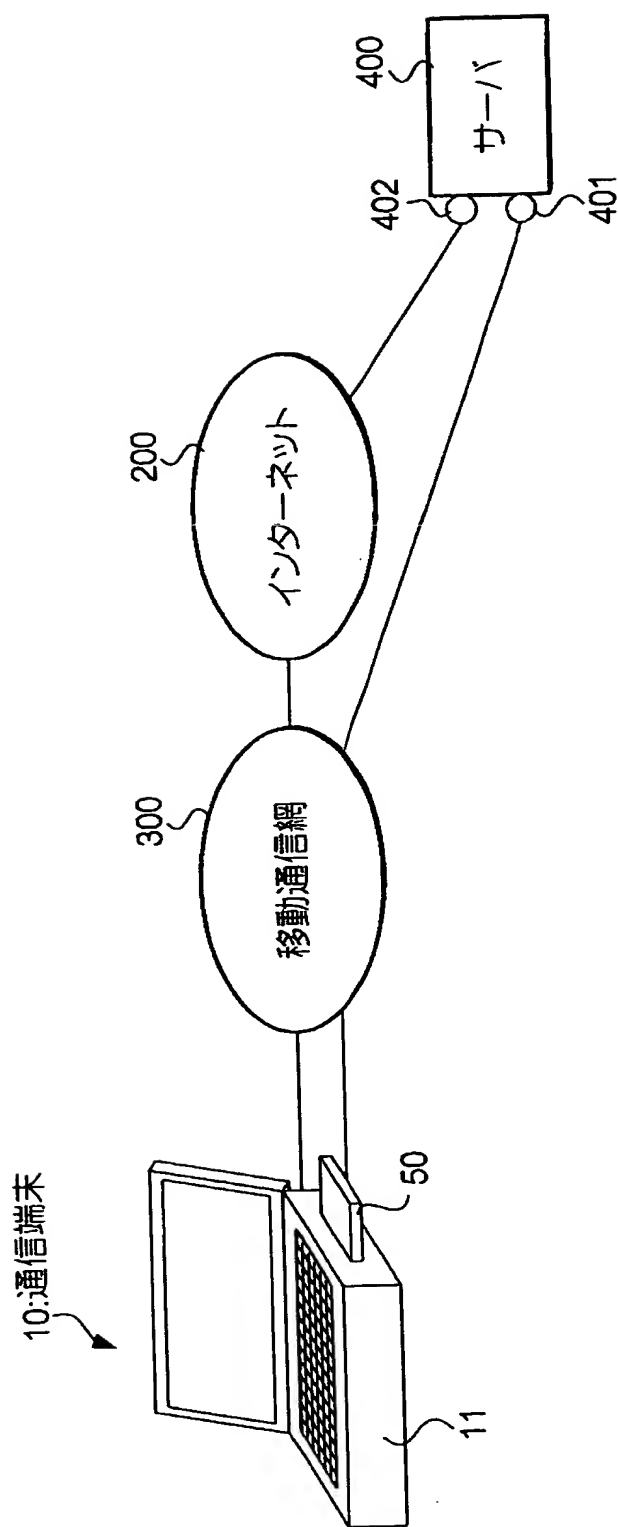
【図9】



【図 10】



【図11】



【書類名】 要約書

【要約】

【課題】 秘匿を必要とする情報の通信を高いセキュリティを維持し、かつ、迅速に行う秘匿を必要とする。

【解決手段】 通信端末 1 0 は、パソコン 1 1 に P C カード 5 0 が装着され、パソコン 1 1 はモデムを介して固定通信網 1 0 0 に接続され、P C カード 5 0 は移動通信網 3 0 0 に接続される。サーバ 4 0 0 の第 1 ポート 4 0 1 は移動通信網 3 0 0 に接続され、第 2 ポート 4 0 2 はインターネット 2 0 0 に接続される。秘匿を必要としない情報は、固定通信網 1 0 0 およびインターネット 2 0 0 を介して通信を行い、秘匿を必要とする情報は、移動通信網 2 0 0 を介した回線で行う。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2000-151879
受付番号	50000634911
書類名	特許願
担当官	佐藤 一博 1909
作成日	平成12年 5月30日

<認定情報・付加情報>

【特許出願人】

【識別番号】

392026693

【住所又は居所】

東京都千代田区永田町二丁目11番1号

【氏名又は名称】

株式会社エヌ・ティ・ティ・ドコモ

【代理人】

申請人

【識別番号】

100098084

【住所又は居所】

東京都中央区日本橋三丁目2番16号 八重洲マ

スヤビル5階 朝日特許事務所

【氏名又は名称】

川△崎▽ 研二

【選任した代理人】

【識別番号】

100111763

【住所又は居所】

東京都中央区日本橋3丁目2番16号 八重洲マ

スヤビル5階 朝日特許事務所

【氏名又は名称】

松本 隆

【選任した代理人】

【識別番号】

100108936

【住所又は居所】

東京都中央区日本橋3丁目2番16号 八重洲マ

スヤビル5階 朝日特許事務所

【氏名又は名称】

秦 貴清

出 願 人 履 歴 情 報

識別番号 [392026693]

1. 変更年月日	2000年 5月19日
[変更理由]	名称変更
住 所	東京都千代田区永田町二丁目11番1号
氏 名	株式会社エヌ・ティ・ティ・ドコモ

This Page Blank (uspto)